any support. As such, it must be based upon Applicant's disclosure, which is explicitly prohibited by the MPEP.

Second, the recitation of determining a security parameter is not the *only* difference between the pending claims and those of the issued patent. For instance, claim 1 recites the step of drawing a random number between 0 and 2^s. Thus, the security parameter establishes the range of numbers from which the random number can be selected. Even if one were to assume that it is obvious to determine a security parameter, *per se*, the Office Action has not shown that it would be obvious to use the security parameter for this purpose.

Claim 1 also recites the step of "calculating the integer d'=d+k*n", where *k* is the random number and *n* has been defined as the number of points of an elliptical curve. In contrast, claim 1 of the '986 patent recites "calculating an integer d' such that d'=d+r", where *r* is a random value with the same size as *d*. The Office Action has not shown where this difference is suggested in the prior art. For instance, where is there a teaching to multiply the random number by the number of points of an elliptical curve before adding the result to *d*?

Claims 6 and 11 recite other distinctive features. For instance, claim 6 recites the steps of calculating p'=p*r, where *p* is a prime number and *r* is a random number, and executing the scalar multiplication operation Q=d.P modulo p'. Claim 11 recites the steps of calculating P'= P+R, where *R* is a random point on the elliptical curve, performing the scalar multiplications Q'=d.P' and S=d.R, and calculating Q=Q'-S. The Office Action has not addressed any of these claimed features. It does not show where they can be found in, or are otherwise are obvious from, the claims of the '986 patent.

For at least the foregoing reasons, the Office Action has not established that the pending claims of the present application are obvious in view of the claims of the '986 patent. Withdrawal of the double patenting rejection is respectfully requested.

Claims 1-15 were rejected under 35 USC § 103, on the grounds that they were considered to be unpatentable over the article by Jerome A. Solinas entitled "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", in view of the Curiger et al patent (US 6,064,740). The pending claims are directed to countermeasures against attacks on cryptographic operations, particularly those which are based upon elliptical curves. These countermeasures are effected by introducing a measure of randomness to the operations, so that the same calculation is not carried out every time the cryptographic algorithm is executed. The claims recite that the randomness can be implemented with the private key *d*,

the calculation modulus *p'*, and the point P on the curve to which the scalar multiplication operation is applied.

The Solinas article is directed to elliptic scalar multiplication operations. Other than a brief mention that public-key protocols are based on elliptic curves, the article does not address the field of cryptography. In particular, it does not describe countermeasures to guard against attacks on public key cryptographic systems. Rather, the focus of the Solinas article is making the scalar multiplication more *efficient*.

Since it does not address countermeasures against attacks, the Solinas article does not disclose the features recited in the pending claims. For example, claim 1 recites the steps of drawing a random number *k*, and calculating the integer d'=d+k*n, where *n* is the number of points on an elliptical curve. The Office Action asserts that the Solinas article teaches these claimed steps, but Applicant is unable to find any support for this assertion. The Office Action cites the Solinas article at pages 360 and 361, with specific reference to Algorithms 2 and 3. However, neither of these algorithms relates to the selection and use of random numbers in the calculation of Q=d.p (or Q=n.P in the nomenclature of the Solinas article). If the rejection is not withdrawn, the examiner is requested to identify where the Solinas article teaches the specific steps of (1) determining a security parameter *s*, (2) drawing a random number *k* between 0 and 2^s, and (3) calculating the integer d'=d+k*n, where *n* is the number of points on the elliptical curve.

The Curiger patent was cited for its disclosure of using a microprocessor core to perform modular calculations. However, the Curiger patent does not contain any teachings that overcome the differences between the subject matter of claim 1 and the Solinas article that are identified above. While the Curiger patent is concerned with attacks on cryptosystems, it is not directed to cryptosystems that are based upon elliptical curves. Rather, it deals with operations that are characteristic of Diffie-Hellman and RSA encryption techniques. See, for example, column 2, lines 1-8.

More significantly, the Curiger patent does not disclose the use of random numbers to modify one or more of the parameters of the encryption or decryption algorithm. Instead, its approach to countering attacks is to "normalize" the modular math calculations, so that the timing and power requirements of the calculations are the same, regardless of whether the bit being processed is a one or a zero. See column 3, lines 38-40. As such, it does not disclose the above-noted features of claim 1 that are missing from the Solinas article.

Accordingly, it is respectfully submitted that the subject matter of claim 1 is not rendered unpatentable by the Solinas article, whether considered by itself or in combination with the Curiger patent. For similar reasons, independent claims 6 and 11 are likewise patentable over the teachings of these references. For instance, claim 6 recites the steps of drawing a random number *r*, calculating p'=p*r, and performing the scalar multiplication operation Q=d.P modulo p'. Claim 11 recites the steps of drawing a random point *R* on the elliptical curve, calculating P'= P+R, performing the scalar multiplications Q'=d.P' and S=d.R, and calculating Q=Q'-S. It is noted that the Office Action does not address any of these claimed steps in the rejection of the claims. Nor is it apparent how the Solinas article could be interpreted to disclose them. As such, the Office Action has not established a *prima facie* case of obviousness upon which a proper rejection can be based.

The dependent claims recite additional distinquishing features of the invention. In view of the fundamental differences identified above, it is believed that a detailed discussion of these additional distinctions is unnecessary at this time.

For the foregoing reasons, it is respectfully submitted that all pending claims are patentably distinct from the Solinas article and the Curiger patent, whether considered individually or in combination. Reconsideration and withdrawal of the rejection is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: February 28, 2006

By: Martin E Miller Reg no. 56022
for James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620